UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/597,003	07/06/2006	Gil Sever	P-9541-US	4617

49443 7590 09/29/2011
Pearl Cohen Zedek Latzer, LLP
1500 Broadway
12th Floor
New York, NY 10036

EXAMINER	
ANDERSON, MICHAEL D	
ART UNIT	PAPER NUMBER
2433	
NOTIFICATION DATE	DELIVERY MODE
09/29/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USPTO@pczlaw.com
Arch-USPTO@pczlaw.com

Office Action Summary	**Application No.** 10/597,003	**Applicant(s)** SEVER ET AL.	
	Examiner MICHAEL D. ANDERSON	**Art Unit** 2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2011*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-37* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)□ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-37* is/are rejected.

8)□ Claim(s) _____ is/are objected to.

9)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)□ The specification is objected to by the Examiner.

11)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Remarks

1. Pending claims for reconsideration are **claims 1-37**. Applicant has amended claim 1.

Response to Arguments

2. Applicant's arguments filed 7/05/2011 have been fully considered but they are not persuasive.

In the remarks, applicant argues in substance:

a. ***That-*** Richmond is directed to controlling usage of network resources but is unrelated to protecting, managing or controlling transfer of information between a computer and an external device connected to the computer (pg.1).

In response to applicants argument- *MPEP 2131.05 states that when a rejection is made under 35 U.S.C. 102, as this one is, "arguments that the alleged anticipatory prior art is nonanalogous art or teaches away from the invention... are not germane to a rejection under section 102 ... the reference is still anticipatory if it explicitly or inherently discloses every limitation recited in the claims."* Therefore applicant's argument that Richmond controlling usage of network resources but is unrelated to protecting, managing or controlling transfer of information between a computer and an external device connected to the computer is not persuasive, as examiner believes (as is explained below) that Richmond does teach the claimed limitations.

b. ***That-*** Neither in paragraphs [0047]-[0048] nor elsewhere does Richmond teach, or even remotely suggest analyzing data according to a protocol associated with a physical communication port (pg.4).

In response to applicant's argument- Richmond in its broadest reasonable interpretation suggests in paragraph 0048 analyzing data according to a protocol associated with a physical communication port within the rule application logic which applies packet rules to all packets received from a device of the user at the port module

c. ***That-*** Richmond does not teach storing a portion of data communicated between a computer and an external device or, storing a portion of any data communicated. Rather, rules, service abstractions and other information related to communicated data are stored (pg.4).

in response to applicants argument- Richmond clearly teaches storing a portion of data communicated between a computer and an external device or, storing a portion of any data communicated in [Fig.3/item 308] which discloses that the relationship hierarchy is stored for later use within the storage device [Fig.4/item 410].

d. ***That-*** Richmond does not teach at least the elements of "modifying the type of the transportation" (claim 3), "modifying the status of a requested file" (claim 4) or "...the step of modifying the data transportation further comprises correcting the data" (claim 5).

In response to applicants argument- Richmond teaches that a network administrator may configure/modify a packet rule to prevent certain users from using particular applications.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. **Claims 1-37** are rejected under 35 U.S.C. 102(b) as being anticipated by Pub.No.: US 2003/0154380 A1 to Richmond et al (hereafter referenced as Richmond).

Regarding **claim 1**, Richmond discloses "a method for controlling the transfer of data between a computer and an external device connected to a port of the computer"***(process of authentication and authorization of users [par.0255])*** , "the method comprising the steps of: a. receiving, by a module on the computer, a data portion during a data communication session between the computer and the external device"***(packets[Fig.15/item 1502] are received by network entry device [Fig.15/item 1504])*** , "said external device connected to the computer and communicating therewith via a physical communication port"***(network device serving as entry point to communications network where network device includes port module [par.0046])*** ; "b. analyzing, by said module, the data portion according to a protocol associated with the physical communication port"***(authentication logic to authenticate identity where the configuration logic is operative to configure the port module in response to authentication [par.0047] also see rule application logic [par.0048])*** ; "c. determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached, wherein if no decision may be reached on whether to allow said data communication session" ***(rule application logic [par.0048])***, "then storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a next data portion, and if said decision may be reached, then proceeding to step 'd' "***(store the relationship hierarchy of one or more packet rules [fig.3/item 308])***; "d. determining, by the module, based at least in part on said data portion analysis, whether to allow the data communication session, wherein if said data communication session is to be allowed"***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from***

stored user information if it is determined that the stored identification information matches received information [par.0064]) , "then transferring the data portion with data stored in the associated buffer, if any exist, toward or from the physical communication port, and if said data communication session is not to be allowed, then modifying data transportation related to said data communication session"***(port module with port configuration logic to configure port module with one or more packet rules[par.0046]).***

Regarding **claim 2** in view of claim 1, Richmond discloses "wherein the step of modifying the data transportation comprises blocking the transportation" ***(deny Field may store a value indicating whether or not to deny access [par.0131]).***

Regarding **claim 3** in view of claim 1, Richmond discloses "wherein the step of modifying the data transportation comprises modifying the type of the transportation" ***(using deny filed, packet rule may be modified/configured to prevent certain users from using particular applications [par.0131]).***

Regarding **claim 4** in view of claim 1, Richmond discloses "wherein the step of modifying the data transportation comprises modifying a status of a requested file" ***(using deny filed, packet rule may be modified/configured to prevent certain users from using particular applications [par.0131]).***

Regarding **claim 5** in view of claim 1, Richmond discloses "wherein the step of modifying the data transportation comprises correcting the data according to the communication protocol" ***(network administrator may configure a packet rule accordingly [par.0131]).***

Regarding **claim 6** in view of claim 1, Richmond discloses “wherein the physical communication port is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared” ***(It is known within the art that the port must be that of a parallel or series also see [par.0006] which discloses a plurality of physical ports and [par.0005] two or more fiber optic cables).***

Regarding **claim 7** in view of claim 1, Richmond discloses “wherein the physical communication port is a USB port” (***[par.0006] discloses a plurality of physical ports capable of).***

Regarding **claim 8** in view of claim 1, Richmond discloses “wherein the physical communication port is wireless”***(user device maybe connected to the entry port module by any of a variety of transmission media including wireless or wired based medium[par.0192]).***

Regarding **claim 9** in view of claim 1, Richmond discloses “wherein the step of analyzing the data portion further comprising: (i) determining whether additional processing based on a higher level protocol is required’***([Fig.13b/item 1324], the packet comes to a state to process if the Packet contains a VLAN header)*** , “wherein if additional processing is not required, then continuing at step 'c'” ***([Fig.13b/step c, also see [Fig.13c] shows that if additional processing is not required step C will forward packet based on vlan header [Fig.13c/item 1336])*** , “otherwise continuing at step (ii); and (ii) processing part of the data portion relevant to the higher level protocol according to the higher level protocol and returning to step (i)” ***([Fig.13b/step c, also see [Fig.13c]***

shows that if additional processing is not required step C will forward packet based on vlan header [Fig.13c/item 1336])

Regarding **claim 10**, in view of claim 9, Richmond discloses “wherein the step of analyzing the data portion comprises analyzing relevant to a higher level protocol that is associated with the external device”***(port processing logic maybe configured to forward configured packet through port connecting medium and port module to another destination on the network[par.0249]).***

Regarding **claim 11**, in view of claim 10, Richmond discloses “wherein the data communication session is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols”***(types of devices may include but are not limited too PDA’s , Blackberry, laptops, personal computers [par.0016]).***

Regarding **claim 12**, in view of claim 1, Richmond discloses “wherein the step of analyzing the data portion is performed in respect of the data stored in the associated buffer” ***(store the relationship hierarchy of one or more packet rules [fig.3/item 308).***

Regarding **claim 13**, in view of claim 1, Richmond discloses “wherein the step of determining whether a decision on the data communication session may be reached is performed in respect of the data stored in the associated buffer”***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from stored user information if it is determined***

that the stored identification information matches received information [par.0064]).

Regarding **claim 14**, in view of claim 1, Richmond discloses "wherein the step of determining whether to allow the data communication session is performed in respect of the data stored in the associated buffer"***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from stored user information if it is determined that the stored identification information matches received information [par.0064])***.

Regarding **claim 15**, in view of claim 1, Richmond discloses "wherein the step of receiving a data portion comprises receiving a data portion selected from a group consisting of packet and SCSI block" ***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from stored user information if it is determined that the stored identification information matches received information [par.0064])***.

Regarding **claim 16**, in view of claim 1, Richmond discloses "wherein the step of receiving the data portion comprises obtaining the data portion by emulating a class driver", ***i.e. receiving data portion via hardware device driver that can operate large number of different devices of a similar type (switching device, also general purpose computer which maybe configured to operate as a switching device [par.0006] also see multiple program applications inclusive of driver applications [par.0026]).***

Regarding **claim 17**, in view of claim 1, Richmond discloses " wherein step of receiving the data portion comprises obtaining the data portion by emulating a filter module"***(entry port module maybe configured to apply filtering rules in accordance with IEEE 802.1D based on VLAN specified in the header [par.0205]).***

Regarding **claim 18**, in view of claim 1, Richmond discloses "wherein the step of analyzing the data portion according to a protocol associated with the physical communication port further comprises: i. parsing the data portion; ii. reassembling the data; and iii. analyzing the reassembled data",***(port module with one or more packet rules including user and port configuration logic to configure port module with packet rules and an authentication module to determine the assigned role of user based on identification information[par.0062***]).

Regarding **claim 19**, in view of claim 1, Richmond discloses "wherein the step of determining whether to allow the communication session comprises reviewing a security policy" ***(rule application logic [par.0048])***.

Regarding **claim 20**, in view of claim 1, Richmond discloses "wherein the step of determining whether to allow the communication session comprises examining the working environment in which the computer is operating and allowing the communication only if said computer is operating in one or more of certain working environments"***(physical port receives a packet from a device used by the user and rule application logic to apply one or more packet rules to the received packet before using any of the network resources of***

the network device [par.0052]).

Regarding **claim 21**, Richmond discloses “a system for -computer protecting the transfer of data between a computer coupled to a private network and an external device” ***(process of authentication and authorization of user data [par.0255])***, “the system comprising: a client agent installed on the computer, the client agent having an associated security policy”***(port configuration logic to configure the port module with one or more packet rules corresponding to the user [par.0046])*** ; “a security manager communicatively coupled to the private network and operable to associate said security policy with the client agent”***(authentication module[Fig.15/item1506] also see rule database [Fig.15/iem 1514]); “***wherein the client agent is operative to: obtain at least a portion of a data transfer between a hardware device connected to the computer through a physical communication port of the computer” ***(physical port receives a packet from a device used by the user and rule application logic to apply one or more packet rules to the received packet before using any of the network resources of the network device [par.0052])***; “analyze said at least a portion of the data transfer according to a communication protocol associated with the physical communication port” ***(authentication logic to authenticate identity where the configuration logic is operative to configure the port module in response to authentication [par.0047] also see rule application logic [par.0048])***; “and determine whether the data transfer is allowable based, at least on the analysis of the at least a portion of the data transfer and the security policy” ***(rule application logic***

[par.0048]), "and, if not determining whether the data transfer is allowable, then store the at least portion of the data transfer in a buffer associated with the data transfer and wait for a subsequent data portion and" ***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from stored user information if it is determined that the stored identification information matches received information [par.0064])***, "if determining the data transfer is allowable, then transferring the at least a portion of the data transfer with data stored in the associated buffer, if any exist, toward or from the physical communication port"***(Port module with port configuration logic to configure port module with one or more packet rules [par.0046]).***

Regarding **claim 22** in view of claim 21, Richmond discloses "wherein the security manager is operable to verify that the security policy is correct" ***(authentication module[Fig.15/item1506] also see rule database [Fig.15/iem 1514]).***

Regarding **claim 23** in view of claim 21, Richmond discloses "wherein the security policy includes a plurality of rules that at least define limits on data transfers during a communication session" ***(authentication module[Fig.15/item1506] also see rule database [Fig.15/iem 1514]).***

Regarding **claim 24** in view of claim 21, Richmond discloses "wherein the security policy includes a plurality of rules related to that at least a content of the data portion and define the a type of an operation that can be performed during communication session" ***(authentication module[Fig.15/item1506] also see***

rule database [Fig.15/iem 1514]).

Regarding **claim 25** in view of claim 21, Richmond discloses “wherein the security manager is operable to disable any communication with the computer unless the client agent associated with the computer is active” ***(deny/disable field [par.0131])***

Regarding **claim 26** in view of claim 21, Richmond discloses “wherein the physical communication ports is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared” ***(It is known within the art that the port must be that of a parallel or series also see [par.0006] which discloses a plurality of physical ports and [par.0005] two or more fiber optic cables).***

Regarding **claim 27** in view of claim 21, Richmond discloses “wherein the physical communication ports is a USB port” ***([par.0006] discloses a plurality of physical ports capable of).***

Regarding **claim 28** in view of claim 21, Richmond discloses “wherein the physical communication port is wireless” ***(user device maybe connected to the entry port module by any of a variety of transmission media including wireless or wired based medium[par.0192]).***

Regarding **claim 29** in view of claim 21, Richmond discloses “wherein the client agent is associated with the security policy by loading the security policy into the client agent” ***(physical port must receive/load from a device used by the user and rule application logic to apply one or more packet rules to the received packet before using any of the network resources [par.0052]).***

Regarding **claim 30** in view of claim 21, Richmond discloses “wherein the security manager is operable to verify that the security policy loaded into the client agent has not been modified” ***((authentication module[Fig.15/item1506] also see rule database [Fig.15/iem 1514]).***

Regarding **claim 31** in view of claim 21, Richmond discloses “wherein the client agent is further operative to transmit a report to a security server, the report identifying events that occurred with the computer in view of the security policy”***(user information about the user is stored on a computer readable medium residing on communication network [par.0067]).***

Regarding **claim 32** in view of claim 21, Richmond discloses “wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with the hardware device, wherein the hardware device is selected from a group consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle” ***(port processing logic maybe configured to forward configured packet through port connecting medium and port module to another destination on the network[par.0249] additionally (types of devices may include but are not limited too PDA’s , Blackberry, laptops, personal computers [par.0016]).***

Regarding **claim 33** in view of claim 21, Richmond discloses “wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols" ***(port processing logic maybe configured to forward configured packet through port connecting medium and port module to another destination on the network[par.0249] additionally (types of devices may include but are not limited too PDA's , Blackberry, laptops, personal computers [par.0016]).***

Regarding **claim 34**, Richmond discloses "a computer having installed thereon a module operative to: obtain at least a portion of a data transfer passing through at least one physical communication port of the computer" ***(port configuration logic to configure the port module with one or more packet rules corresponding to the user [par.0046])***; "analyze said at least a portion of the data transfer according to a communication protocol associated with the at least one physical communication port" ***(authentication logic to authenticate identity where the configuration logic is operative to configure the port module in response to authentication [par.0047] also see rule application logic [par.0048])***; "and determine whether the data transfer is allowable based:, at least in part, on the analysis of the at least a portion of the data transfer and a security policy" ***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from stored user information if it is determined that the stored identification information matches received information [par.0064])***, "and, if not determining whether the data transfer is allowable, then store the at least portion of the data transfer in a buffer associated with the data transfer and wait for a subsequent data portion and, if determining the data transfer is allowable, then transferring the at least a portion of the data transfer with data stored in the associated buffer, if any exist, toward or from the physical communication port" "***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from stored user information if it is determined that the stored identification information matches received information [par.0064]).***

Regarding **claim 35** in view of claim 10, Richmond discloses "wherein the device is a device selected from a group of devices consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle" ***(types of devices may include but are not limited too PDA's, Blackberry, laptops, personal computers [par.0016]).***

Regarding **claim 36** in view of claim 1, Richmond discloses "wherein determining whether a decision on whether to allow the data communication session may be reached is based on at least two data portions wherein at least one of said two data portions is stored in said buffer"***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from stored user information if it is determined that the stored identification information matches received information [par.0064]).***

Regarding **claim 37** in view of claim 1, Richmond discloses "wherein determining whether to allow the data communication session is based on at least two data portions wherein at least one of said two data portions is stored in said buffer" ***(authentication module controls accessing stored user information to determine if the identification matches that of received packet, and to determine assigned role from stored user information if it is determined that the stored identification information matches received information [par.0064]).***

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL D. ANDERSON whose telephone number is (571)270-5159. The examiner can normally be reached on Monday-Friday 8am til 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, VIVEK SRIVASTAVA can be reached on (571)272-7304. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MICHAEL D. ANDERSON
Examiner, Art Unit 2433

/VIVEK SRIVASTAVA/

Supervisory Patent Examiner, Art Unit 2433